Samuel Dupuis
212168001

Unfair Teams:
Imbalanced Races amongst Products of Primes

Introduction: What are primes, and where are they?

The prime numbers are those positive integers (1,2,3…) which are divided without remainder by precisely two other positive integers: one and themselves. For instance, six is not prime because two and three divide it, but seven is prime because no positive integers other than seven and one divide it. Among all the numbers with which we count positive whole quantities, the integers, we have long understood that the primes have great theoretical importance and practical use. Leaving aside the particular uses of primes and formulas which apply to some or all of them, their study has included questions of what patterns they form or rules they obey as groups of numbers rather than individually. The foundational result in this line of thinking is due to Euclid, who showed over two thousand years ago that there are infinitely many prime numbers; since this result, endless patterns have been found concerning about how primes and integers related to prime formulas are distributed on the number line.

When we speak of one infinite subset of the positive integers being 'larger' than another, what we really mean is that as we count up the members of both sets starting at 0 up to some counting variable x, the 'larger' set will generally count up faster than the other one. These counts are the **counting functions** of each set. Strictly speaking both sets, as far as the infinite goes, are still in their totality the same sort of infinitely large (an infinite subset of the integers).

The Prime Number Theorem in Arithmetic Progressions and Chebyshev's Bias

Consider dividing all the positive integers into equally sized consecutive groups of length four. Start with zero, one, two and three; then the next group is four, five, six, seven, and so on. So the first slots in each group are the multiples of four, the second are multiples of four plus one, then plus two, then plus three. Integers *n* of each type are then said to be in the **residue class modulo 4** or simply **mod 4** of their remainder when *n* is divided by four (which is that quantity that you add to the multiple of four just less than *n*).

Since Euclid's famous proof of his theorem we have known that there are infinitely many prime numbers with remainder either one or three modulo four; all numbers in the other classes are even, so the only prime number in those classes is two. De la Vallée-Poussin proved in the late 1800s that the classes 1 and 3 mod 4 have infinitely many primes in them, and as one searches out to infinity the ratio between the number of primes one finds in each class approaches 1. This result was in fact proved for all residue classes *a* mod *k* for any positive integer *k* with 0 ≤ *a* < *k* and *a* **coprime** to *k*; this is to say that only 1 divides *a* and *k*. This means that, for each *k*, all coprime **residue classes** *a* share as many primes as each other more or less equally as one considers the shares of each residue class of primes below a given value *x* and then *x* is taken to infinity. This statement is a key part of **the prime number theorem in arithmetic progressions.**

While it may be true that the ratio between the primes shared between any such permissible classes tends to 1 as one considers larger and larger upper bounds for counting the primes, Chebyshev observed an imbalance for lower values. **Chebyshev's bias**, in particular, refers to the observed faster accumulation of primes in the counting function of the primes in the residue class 3 mod 4 over 1 mod 4. Despite this phenomenon having been observed more than 150 years ago, a proof of the modern forms of the bias (for other residue classes) that hold out to infinity is thought to be extremely difficult, and for now the trend is simply taken for granted for small numbers and thought to be a true (but unproven) statement for the whole counting functions.

Analytic Number Theory: In Which Riemann Spilled Complex Analysis on the Integers and it was Good

The aforementioned proof of the prime number theorem in arithmetic progressions (and the proof of the original prime number theorem) both included, in their early forms, the extended calculus over the complex numbers: **complex analysis**. Bernhard Riemann had this insight in 1859, with the publication of his one and only manuscript on number theory. He introduced his famous function, the **Riemann zeta function**, and made his conjecture (the **Riemann hypothesis**) which to this day is without resolution and intensely studied in the mathematical community.

Riemann's core insight was to find a connection between his zeta function and another function related to the logarithms of primes at their powers, the **second Chebyshev function**. This function and the **prime counting function** itself, together with the **first Chebyshev function** (which includes the logarithms of the primes only at themselves), are closely enough related that statements about some of them translate into related statements about others. It was then through this somewhat roundabout route, asking a question about the zeta function which led to the second Chebyshev function and finally to the prime counting function that de la Vallée-Poussin was able to prove the prime number theorem. From this time forward, number theory has been influenced greatly by its analytic sector due to the ongoing success of these ideas.

The connection is especially striking given that the relevant statements about the zeta function (here, that it is never zero when its argument has real part one or zero) are statements about continuous regions and generally solved using calculus. But how do continuous functions and their behaviors have anything to do with the structure of prime numbers, which exist in the discrete and orderly structure of the integers? How do we reach statements about the placement of these points from integrals and derivatives? It turns out that there are several ways to use the fact that the integers live in the real numbers, and don't necessarily need to be viewed in isolation, to 'connect the dots' by showing that integer functions are related to real, smooth curves that look much like them. We then move from real curves in the x-y plane of real numbers to the complex realm via discoveries of the early and middle 19th century, where real curves are again viewable as slices of much richer four dimensional functions from the complex numbers to themselves (the w-z 4-dimensional space).

Working in the space of the discrete functions related to primes, it turns out that there is a great deal of randomness on a fine level even as they are well approximated by continuous counterparts. Formally, we tend to contain this randomness in **error terms,** functions which are the differences between an ideal smooth model and the actual discrete prime-related function of interest. These error terms are themselves typically expressed in **big oh** and **small oh** notation, which indicate that the size of the error does not exceed a particular bounding function by more than a multiplicative factor when sufficiently far from zero. For instance, f(x) = O(log(x)) tells us that when x is large enough (greater than some value y), the magnitude of f(x) does not exceed some multiple of log(x) at any x > y.

References

[1] Riemann. Translated by David Wilkins. URL: http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/EZeta.pdf. 1857. Accessed February 23rd, 2017.

[2] Dummit, Granville, and Kisilevsky. "Big Biases Amongst Products of Two Primes". URL: arXiv:1411.4594v1. 2014. Accessed: August 10th 2016.

[3] Dupuis. "Survey of Big Biases Amongst Products of Two Primes". 2016.

[4] Hildebrand. "Introduction to Analytic Number Theory; Math 531 Lecture Notes". 2005.

The Punchline: Products of Two Primes

Despite the difficulty of proving that Chebyshev's bias is a real effect out to infinity, a paper was written in 2014 by David Dummit, Andrew Granville and Hershy Kisilevsky in which a similar bias was proved to exist for *products of two or more prime numbers* without relying on unresolved conjectures. The work done here was a survey and explicit calculation of what was done in this paper. The formal result was, in the case of only two prime numbers [2]:

Theorem 1.1. *Let χ be a quadratic character of conductor d. For $\eta = -1$ or 1 we have*

$$\frac{\#\{pq \le x : \ \chi(p) = \chi(q) = \eta\}}{\frac{1}{4}\#\{pq \le x : \ (pq, d) = 1\}} = 1 + \eta\frac{(\mathcal{L}_\chi + o(1))}{\log\log x} \quad \textit{where} \quad \mathcal{L}_\chi := \sum_p \frac{\chi(p)}{p}.$$

This is a much more general statement outside of the residue classes of 4, but in the case of 4 there is only one X (chi) function; this is 0 at 2 and 4, equal to 1 at 1, -1 at 3, and periodic with period 4. Briefly, these chi functions (the **quadratic characters** in question) are functions that are 1 or -1 at values coprime to the residue class. An important quadratic character that exists for all residue classes (or **modulo** a period n, with the least period being the **conductor**) is the indicator of whether or not a square can be equal to that residue, when the residue is coprime to the period. This indicator is then 1 on the square candidates, and -1 on the squareless residues. The direction and value of the biases for given X then depend on the sign and magnitude of L_X, which in the case of the lone quadratic character modulo 4 is about -0.334.

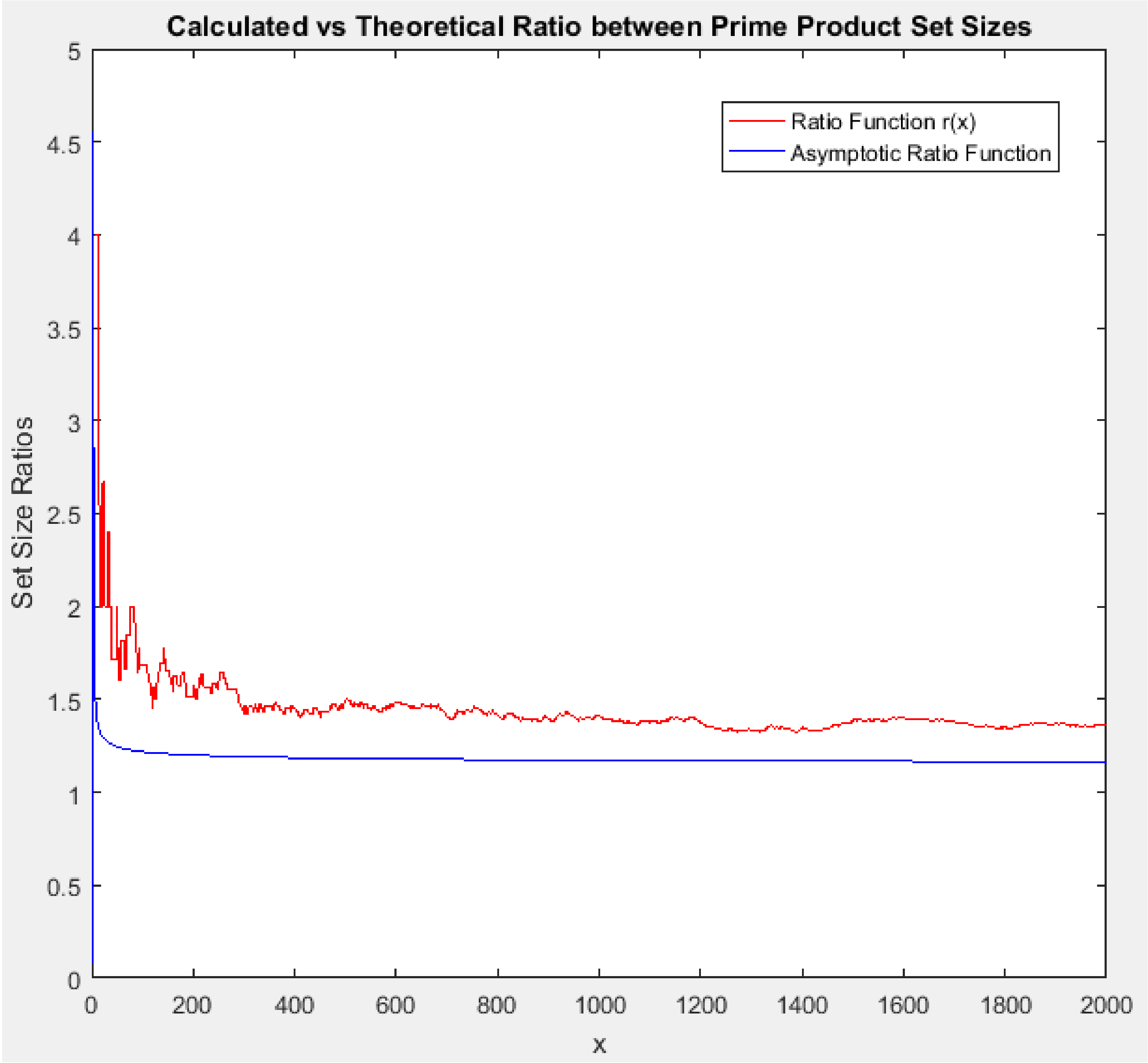
In the case of conductor 4, we then consider that there are four possibilities for (most) products of two primes: both prime factors are congruent to 3, one is congruent to 3 and one is congruent to 1 (this is two groups when we consider that one prime is larger and one is smaller, usually) and then finally both primes may be congruent to 1. Going to infinity, each of these groups would approach the same size very quickly if the weighted sum of congruences for primes L_X was zero; however, the fact that this sum is usually not zero actually introduces a very appreciable imbalance between the sizes of each of these sets out to infinity. With our value of -0.334 and given that X(3) = -1, then more products of two primes end up with two prime factors congruent to 3 mod 4 much more than a quarter of the (naively expected) uniformly distributed case.

(More) Technical Notes

What follows are some techniques that were used to clarify the calculations in [2], present explicitly in [3].

Partial Summation is a technique of splitting sums over the integers of pointwise products of functions, at least one of which must be a restriction of a smooth function to the integers, into sums and integrals involving those two functions split apart into products [4]. The use of this technique is to disentangle a difficult sum of a product of two simpler functions, and express this sum in terms of operations on the pieces. In this case, there are many sums of logarithms and powers of prime numbers; partial summation splits these logarithms and powers into their own functions of x, and the prime identifying function as the function which is 1 when an integer n is prime and 0 when the argument n is composite. Each of those functions is more manageable by themselves, but together in a sum they are more difficult to bound together without this tool.

Small oh notation, unlike big oh, describes a stronger bound in terms of the sample function. Where big oh bounds imply that the bounded function does not exceed a factor of the bounding function, small oh notation implies that the bounded function must become very small compared to the bounding one. Even though small oh is the stronger statement, it usually implies that there is an even better big oh bound available; therefore, small oh bounds are often viewed as provisional bounds to be improved upon with more intense scrutiny.



Comparison of the left hand side of Theorem 1 (in red) to the function on the right without the shift that goes to zero (the o(1) term). The functions only become fairly close as x goes beyond around ten million.